(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Off nl gungsschrift**

(10) **DE 42 17 830 A 1**

(51) Int. Cl.[5]:
G 06 F 1/30
G 06 F 12/16
G 07 B 17/00

(21) Aktenzeichen: P 42 17 830.4
(22) Anmeldetag: 29. 5. 92
(43) Offenlegungstag: 2. 12. 93

DE 42 17 830 A1

(71) Anmelder:
Francotyp-Postalia GmbH, 13409 Berlin, DE

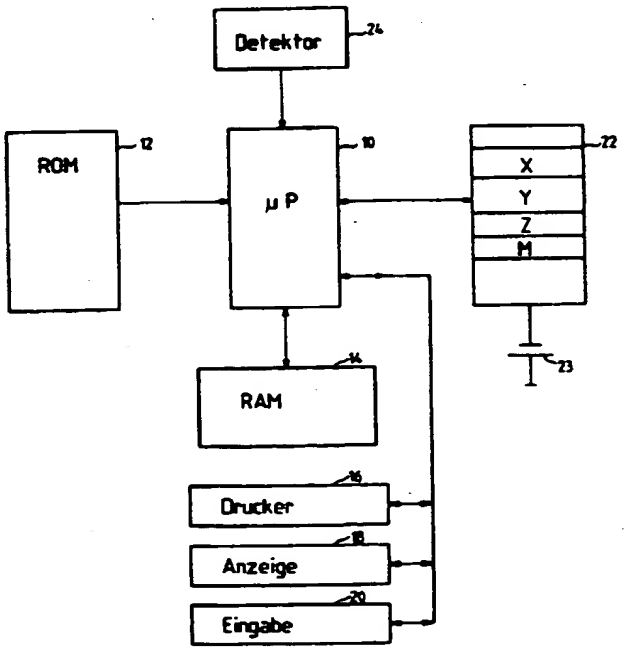
(74) Vertreter:
Schaumburg, K., Dipl.-Ing.; Thoenes, D., Dipl.-Phys. Dr.rer.nat., Pat.-Anwälte, 81679 München

(72) Erfinder:
Günter, Stephan, 1000 Berlin, DE

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Betreiben einer Datenverarbeitungsanlage

(57) Beschrieben wird ein Verfahren zum Betreiben einer Datenverarbeitungsanlage, bei dem ein kritischer Programmabschnitt abgearbeitet wird, der das Einschreiben von Informationen in einen ersten nicht flüchtigen Speicher (X) veranlaßt. Bei einer auf einen Spannungsausfall folgenden Spannungswiederkehr werden die vor dem Spannungsausfall im Speicher (X) vorhandenen Informationen wieder bereitgestellt. Zu Beginn des Einschreibens der Informationen wird eine erste Zustandskennung in einen Zustandsspeicher (Z) einmal eingeschrieben und nach dem Einschreiben der Informationen eine zweite Zustandskennung in den Zustandsspeicher (Z) eingeschrieben. Danach werden dieselben Informationen in einen zweiten nicht flüchtigen Speicher (Y) eingeschrieben. Bei Spannungswiederkehr wird die zuletzt eingeschriebene Zustandskennung gelesen. Bei Vorliegen der ersten Zustandskennung werden die Informationen aus dem zweiten Speicher (Y) in den ersten Speicher (X) übertragen. Bei Vorliegen der zweiten Zustandskennung werden die Informationen aus d m ersten Speicher (X) in den zweiten Speicher (Y) eingelesen.



DE 42 17 830 A1

Beschreibung

Die Erfindung betrifft ein Verfahren zum Betreiben einer Datenverarbeitungsanlage, bei dem die Datenverarbeitungsanlage mindestens inen kritischen Programmabschnitt abarbeitet, der das Einschreiben von Informationen in einen ersten nicht flüchtigen Speicher veranlaßt und der nach erfolgter Abarbeitung verlassen wird, wobei bei einer auf einen Spannungsausfall folgenden Spannungswiederkehr die vor dem Spannungsausfall im Speicher vorhandenen Informationen wieder bereitgestellt werden.

Ein derartiges Verfahren wird z. B. bei einer Frankiermaschine eingesetzt, die einen nicht flüchtigen Speicher hat, in dem die noch verfügbaren Portobeträge oder die bereits aufgebrauchten Portobeträge gespeichert werden. Bei Spannungswiederkehr nach einem Spannungsausfall muß der Inhalt des Speichers für die weiteren Buchungsvorgänge mit dem Inhalt vor dem Spannungsausfall übereinstimmen.

Bei einem aus der US-A 45 06 299 bekannten Verfahren erzeugt ein Spannungsüberwachungsschaltkreis beim Absinken der Versorgungsspannung ein Signal, welches eine Speichersicherungsroutine in der Datenverarbeitungsanlage auslöst, bei der die sicherheitsrelevanten Informationen in einen nicht flüchtigen Speicher eingeschrieben werden. Um die Routine auch bei abrupt fehlender Versorgungsspannung noch ausführen zu können, muß eine Energiereserve vorgesehen werden, beispielsweise in Form einer in einem Kondensator gespeicherten elektrischen Ladung, die die Betriebsfähigkeit der Datenverarbeitungsanlage über den Zeitpunkt des Spannungsausfalls hinaus für kurze Zeit verlängert. Wenn die Versorgungsspannung wiederkehrt, wird eine weitere Routine gestartet, welche die im nicht flüchtigen Speicher zwischengespeicherten Informationen wieder bereitstellt.

Nachteilig beim bekannten Verfahren ist das Erfordernis, spezielle Hardwarekomponenten zum Erkennen des Absinkens der Versorgungsspannung sowie zur verlängerten Energieversorgung vorzusehen. Dies bedeutet, daß in die Hardware konventioneller Rechnerbaugruppen eingegriffen oder diese Hardware um weitere Bauelemente ergänzt werden muß, um eine Speichersicherung zu erreichen. Der damit verbundene technische Aufwand könnte vermieden werden, wenn es gelänge, die mit der Hardware erreichten Wirkungen durch Lösungen im Softwarebereich zu erzielen.

Es ist Aufgabe der Erfindung, ein Verfahren zum Betreiben einer Datenverarbeitungsanlage anzugeben, das mit geringem Hardwareaufwand realisiert werden kann und einen hohen Sicherheitsstandard gewährleistet.

Diese Aufgabe wird für ein eingangs genanntes Verfahren dadurch gelöst, daß zu Beginn des Einschreibens der Informationen eine erste Zustandskennung in einen nicht flüchtigen Zustandsspeicher mindestens einmal eingeschrieben wird, daß nach dem Einschreiben der Informationen eine zweite, von der ersten Zustandskennung verschiedene Zustandskennung in den Zustandsspeicher mindestens einmal eingeschrieben wird, die selben Informationen in einen zweiten nicht flüchtigen Speicher eingeschrieben werden und der kritische Programmabschnitt verlassen wird, daß bei Spannungswiederkehr die vor dem Spannungsausfall in den Zustandsspeicher zuletzt eingeschriebene Zustandskennung gelesen wird und bei V rliegen der ersten Zustandskennung diese in den Zustandsspeicher mindestens einmal eingeschrieben wird, die Informationen aus

dem zweiten Speicher in den ersten Speicher übertragen werden und der kritische Programmabschnitt verlassen wird, und daß bei Vorliegen der zweiten Zustandskennung diese in den Zustandsspeicher mindestens einmal eingeschrieben wird, die Informationen aus dem ersten Speicher in den zweiten Speicher eingelesen werden und der kritische Programmabschnitt verlassen wird.

Die Erfindung beruht auf der Überlegung, die zu sichernden Informationen zweimal in voneinander getrennten nicht flüchtigen Speichern abzulegen. Fällt die Versorgungsspannung zu einem Zeitpunkt aus, zu dem gerade ein Schreibvorgang im ersten Speicher ausgeführt wird, so ist nicht sichergestellt, daß die zu speichernde Information, z. B. ein Datenbyte, ordnungsgemäß in den Speicher gelangt. Jedoch sind die im zweiten nicht flüchtigen Speicher enthaltenen Informationen, die beim vorherigen Abarbeiten des kritischen Programmabschnitts abgespeichert worden waren, noch unverfälscht erhalten. Die in diesem Speicher gespeicherten Informationen werden nun gemäß der Erfindung in den ersten Speicher eingeschrieben, so daß dessen Speicherinhalt mit dem des zweiten Speichers übereinstimmt. Ein eventueller Schreibfehler im ersten Speicher ist somit aufgehoben.

Wird der kritische Programmabschnitt wegen Spannungsausfalls in der Phase unterbrochen, in der die Informationen in den zweiten Speicher eingeschrieben werden, so wird bei Spannungswiederkehr der Inhalt des ersten Speichers in den zweiten Speicher geladen und so ein möglicher Schreibfehler im zweiten Speicher behoben.

Zur Unterscheidung der verschiedenen Phasen des Einschreibens der Informationen in die beiden Speicher werden diese Phasen jeweils durch eine Zustandskennung gekennzeichnet, z. B. durch eine Zahl oder ein Textzeichen. Bei Spannungswiederkehr wird dann anhand dieser Zustandskennung entschieden, welcher Speicher mit den Informationen des anderen Speichers zu laden ist.

Nach Spannungswiederkehr wird die Phase des Programmabschnitts, in der die Inhalte der Speicher ausgetauscht werden, durch Zustandskennungen gekennzeichnet. Wenn nun in dieser Phase ein Spannungsausfall auftritt, so wird nach Spannungswiederkehr der noch unverfälscht vorhandene Inhalt des ersten oder des zweiten Speichers in den von der Spannungsunterbrechung betroffenen Speicher übertragen. Dadurch wird für alle möglichen Zeitpunkte einer Spannungsunterbrechung sichergestellt, daß die vor der Spannungsunterbrechung vorhandenen Informationen auch nach Spannungswiederkehr ordnungsgemäß zur Verfügung stehen.

Erfindungsgemäß erfolgt das Einschreiben der Zustandskennungen in den Zustandsspeicher jeweils mindestens einmal. Unter normalen Betriebsbedingungen ist dies zum Erzielen einer hohen Sicherheit ausreichend, da das Einschreiben nur sehr kurze Zeit erfordert und der Betriebszustand, bei dem während des Einschreibens ein Spannungsausfall eintritt und die Zustandskennung nicht ordnungsgemäß in den Zustandsspeicher eingetragen wird, sehr unwahrscheinlich ist. Will man aber diesen seltenen Betriebsfall ebenfalls sicher beherrschen, so sind die Zustandskennungen jeweils mehrfach in den Zustandsspeicher einzutragen. Damit wird erreicht, daß selbst bei einem aktuellen fehlerhaften Eintrag die zuv r eingetragene Zustandskennung noch ermittelt werden kann.

Vorteilhafterweise wird beim Lesen der Zustandskennung nach Spannungswiederkehr diese Kennung für die weitere Auswertung zwischengespeichert und die aktuelle Zustandskennung in die selben Speicherplätze des Zustandsspeichers geschrieben, wie die vorherige Zustandskennung, d. h. die Speicherinhalte werden unmittelbar ersetzt. Eine andere Möglichkeit ist die rollierende Eintragung der Zustandskennung in den Zustandsspeicher, wobei die aktuelle Zustandskennung in die Speicherzelle mit gegenüber dem letzten Eintrag z. B. um 1 erhöhter Adresse abgespeichert wird. Wenn so weiter verfahren wird und ein definierter Speicherbereich des Zustandsspeichers vollständig beschrieben ist, wird dieser Bereich des Zustandsspeichers von vorne beginnend überschrieben. Auf diese Weise bleiben die zuletzt eingetragenen Zustandskennungen für eine gewisse Zeit noch gespeichert, so daß auf diese zur Auswertung zugegriffen werden kann.

Die benötigten Speicher, d. h. der erste, zweite Speicher und der Zustandsspeicher können räumlich voneinander getrennt vorhanden sein. Es ist aber auch möglich, nur einen einzigen nicht flüchtigen Speicher vorzusehen, der in verschiedene Speicherbereiche eingeteilt ist, die als die vorgenannten Speicher dienen.

Eine bevorzugte Weiterbildung der Erfindung ist dadurch gekennzeichnet, daß die Datenverarbeitungsanlage mindestens einen unkritischen Programmabschnitt abarbeitet, der kein Einschreiben von Informationen in den ersten oder zweiten nicht flüchtigen Speicher veranlaßt, wobei zu Beginn des Abarbeitens dieses unkritischen Programmabschnitts in den Zustandsspeicher eine dritte Zustandskennung mindestens einmal eingeschrieben wird, und daß bei Spannungswiederkehr beim Vorliegen der dritten Zustandskennung das Abarbeiten des unkritischen Programmabschnitts beim unterbrochenen Programmschritt fortgesetzt wird.

Bei zahlreichen Anwendungen sind Programmabschnitte vorhanden, die nicht sicherheitsrelevante Informationen in Speichern verändern. Eine solche Anwendung ist z. B. das Berechnen von Zwischenergebnissen oder die Dateneingabe, wobei die erforderlichen Programmschritte jeweils anwendungsspezifisch in einem nicht kritischen Programmabschnitt zusammengefaßt sein können. Durch die Maßnahmen der Weiterbildung wird erreicht, daß bei Spannungswiederkehr unmittelbar zum letzten Programmschritt des unkritischen Programmabschnitts verzweigt wird und dort das Abarbeiten von Programmschritten durch die Datenverarbeitungsanlage fortgesetzt wird.

Eine andere Weiterbildung sieht vor, daß mindestens ein kritischer Programmabschnitt und/oder mindestens ein unkritischer Programmabschnitt Teil eines Programmoduls ist, das von der Datenverarbeitungsanlage abgearbeitet wird. Das Programmodul stellt eine in sich geschlossene Funktionseinheit dar, die beispielsweise bei einer Frankiermaschine das Frankieren oder das Eingeben von Portowerten steuert. Durch diese Maßnahme werden die vorgenannten Programmabschnitte in ein Programmodul eingebunden, beispielsweise in Form von Unterprogrammen oder Makroprogrammen.

Die vorgenannte Weiterbildung kann weiterhin dadurch gekennzeichnet sein, daß nach Spannungswiederkehr und bei Vorliegen der ersten Zustandskennung die vom Programmodul gesteuerten Prozesse zurückgesetzt und/oder das Programmodul erneut abgearbeitet wird.

Durch diese Maßnahme wird erreicht, daß nach Wiederherstellung des Inhalts des ersten nicht flüchtigen Speichers die durch den Spannungsausfall unterbrochene Funktion von Beginn an wiederholt wird. Dadurch wird sichergestellt, daß eine einmal begonnene, aber nicht beendete Funktion, beispielsweise ein Druckvorgang, zuverlässig ausgeführt wird.

Wird dagegen nach Spannungswiederkehr festgestellt, daß der kritische Programmabschnitt mit zweiter Zustandskennung unterbrochen worden ist, so wird das Abarbeiten des Programmoduls nach Verlassen des kritischen Programmabschnitts, in dem der Inhalt des zweiten Speichers in Übereinstimmung mit dem des ersten Speichers gebracht worden ist, fortgesetzt.

Eine andere Weiterbildung ist dadurch gekennzeichnet, daß beim Abarbeiten mehrerer Programmodule jedem Programmodul eine Modulkennung zugeordnet wird, die in einem Modulspeicher zu Beginn des Abarbeitens des Programmoduls mindestens einmal abgespeichert wird, und daß bei Spannungswiederkehr zum Programmodul mit der zuletzt abgespeicherten Modulkennung verzweigt wird.

Durch diese Maßnahme wird erreicht, daß nach Spannungswiederkehr dasjenige Programmodul weiter abgearbeitet wird, das bei Spannungsausfall unterbrochen wurde.

Bei einer weiteren Ausgestaltung der Erfindung wird die erste, die zweite und/oder die dritte Zustandskennung und/oder die Modulkennung jeweils in n Speicherzellen des Zustandspeichers bzw. des Modulspeichers mehrfach abgespeichert, wobei n eine vorgegebene Zahl ist, vorzugsweise 3. Durch das mehrfache Abspeichern der Kennungen wird erreicht, daß die in der Zustandskennung enthaltene Information auch dann noch rekonstruiert werden kann, wenn während des Abspeicherns einer Zustandskennung ein Schreibfehler, z. B. infolge eines Spannungsausfalls auftritt. Die vor diesem Schreibfehler ordnungsgemäß abgespeicherte Zustandskennung kann bei der Spannungswiederkehr ausgewertet werden.

Bei einer Weiterbildung ist vorgesehen, daß bei Spannungswiederkehr die n Speicherzellen des Zustandspeichers bzw. des Modulspeichers gelesen werden, und daß durch eine Majoritätsprüfung und/oder eine Plausibilitätsprüfung festgestellt wird, welche Zustandskennung bzw. Modulkennung vorliegt. Durch diese Maßnahmen wird erreicht, daß bei einem fehlerhaften Abspeichern der letzten Zustandskennung bzw. Modulkennung infolge eines Schreibfehlers die richtige Information noch ermittelt werden kann. Wird z. B. die Zustandskennung ZK = 1 insgesamt 4 mal in 4 verschiedene Speicherzellen des Zustandsspeichers eingetragen (d. h. n = 4) und ist infolge eines Spannungsausfalls beim vierten Eintrag fälschlicherweise ZK = 5 eingetragen worden, so wird bei der Plausibilitätskontrolle festgestellt, daß der Wert ZK = 5 fehlerhaft ist, da dieser Wert nicht innerhalb eines vorgegebenen Wertebereichs liegt. Dagegen werden die Einträge ZK = 1 als gültige Werte erkannt. Als richtige Zustandskennung wird dann ZK = 1 ausgewählt.

Bei der Majoritätsprüfung wird festgestellt, welcher Wert in einem Ensemble von Werten am häufigsten vorkommt. Dieser Wert wird dann als die richtige Zustandskennung interpretiert. Je größer die Zahl n gewählt wird, um so höher ist bei der Majoritätsprüfung die Wahrscheinlichkeit mit der die richtige Zustandskennung festgestellt werden kann. Auf diese Weise ist es möglich, die richtige Zustandskennung bzw. Modulkennung auch dann zu ermitteln, wenn mehrere, aufeinander folgende Schreibfehler infolge eines Spannungsaus-

falls auftreten.

Ein Ausführungsbeispiel der Erfindung wird im folgenden an Hand der Zeichnungen erläutert. Darin zeigen

Fig. 1 das Blockschaltbild einer Frankiermaschine mit Baueinheiten, soweit sie zum Verständnis der Erfindung erforderlich sind,

Fig. 2 ein Flußdiagramm der Startphase nach Spannungswiederkehr,

Fig. 3 ein Flußdiagramm von Programmabschnitten während der Startphase,

Fig. 4 ein Flußdiagramm eines Programmoduls mit kritischen und unkritischen Programmabschnitten, und

Fig. 5 Flußdiagramme betreffend das mehrfache Einschreiben und Lesen von Zustands- bzw. Modulkennungen.

In **Fig. 1** sind in einer Blockdarstellung wichtige Baueinheiten einer Frankiermaschine dargestellt. Ein Mikroprozessor **10** arbeitet das in einem Lesespeicher **12** abgelegte Programm, unterstützt von einem Schreib-/Lesespeicher **14**, ab und steuert einen Frankierdrucker **16**, eine Anzeige **18** sowie eine Dateneingabe **20**. Eine wesentliche Aufgabe des Mikroprozessors **10** ist die Portoabrechnung. Hierzu greift er auf einen zentralen nicht flüchtigen Speicher (**22**) zu, in dem der für die Frankiermaschine noch verfügbare Portobetrag sowie weitere sicherheitsrelevante Daten gespeichert sind. Diese Daten dürfen bei Ausfall der Stromversorgung, z. B. bei Netzausfall oder beim Ausschalten der Frankiermaschine, nicht verloren gehen. Der nicht flüchtige Speicher (**22**) ist daher durch eine Batterie **23** gepuffert, die ihn auch bei Trennung der Frankiermaschine vom Versorgungsnetz für lange Zeit weiter mit Strom versorgt.

Der Speicher **22** ist in verschiedene Speicherbereiche X, Y, Z und M eingeteilt. Der Bereich X entspricht dem weiter oben genannten ersten Speicher, der Bereich Y dem zweiten Speicher, der Bereich Z dem Zustandsspeicher und der Bereich M dem Modulspeicher. Der Zugriff des Mikroprozessors **10** auf diese Bereiche wird weiter unten im Zusammenhang mit dem Verfahrensablauf erläutert.

Ein Spannungsdetektor **24** übermittelt dem Mikroprozessor **10** ein Signal, wenn die Versorgungsspannung der Frankiermaschine ihren normalen Betriebspegel erreicht hat. Ein Detektor, der ein Absinken der Betriebsspannung anzeigt, sowie eine Pufferbatterie, die den Betrieb des Mikroprozessors **10** für kurze Zeit über den Zeitpunkt des Spannungsabfalls hinaus noch aufrechterhält, sind bei der Erfindung nicht erforderlich. Die Komponenten **10**, **12**, **14** und **24** gehören zu den üblichen K mponenten einer Rechnerbaugruppe, so daß bei Anwendung der Erfindung auf derartige Baugruppen zurückgegriffen werden kann und der Hardwareaufbau nicht verändert werden muß.

In **Fig. 2** ist in einem Flußdiagramm der Verfahrensablauf bei Spannungswiederkehr dargestellt. Im Verfahrensschritt **30** wird festgestellt, ob der Detektor **24** eine Spannungswiederkehr meldet. Falls dies zutrifft, wird im Verfahrensschritt **32** das Programmodul SYSTEM abgearbeitet, wobei grundlegende Systemtests durchgeführt werden, beispielsweise, b der nicht flüchtige Speicher (**22**) betriebsbereit ist.

Nach Abarbeiten des Programmoduls SYSTEM wird im Verfahrensschritt **34** das Programmodul START gestartet. Hierzu wird die diesem Programmodul zugeordnete Modulkennung MK in den Bereich M des Speichers **22** eingeschrieben, beispielsweise in Form eines Textes (z. B. "start") oder einer Zahl. Danach wird in den Bereich Z des Speichers **22** die Zustandskennung ZK = 0 eingetragen. Diese Zustandskennung ZK steht für einen nicht kritischen Programmabschnitt, in welchem keine Daten im Speicher **22** geändert werden.

Im nachfolgenden Verfahrensschritt **38** wird ermittelt, ob die vor der Spannungswiederkehr zuletzt eingetragene Zustandskennung ZK den Wert 0 hat. Hierzu wird auf den Bereich Z das Speichers **22** zugegriffen. Wenn dies der Fall ist, d. h. das Programm wurde in einem nicht kritischen Programmabschnitt unterbrochen, so daß eine Wiederherstellung der Speicherinhalte im Speicher **22** nicht erforderlich ist, so wird zum nächsten Programmodul **40** verzweigt, in dem die Initialisierung verschiedener Geräte und Systemkomponenten erfolgt. Anschließend werden die weiteren Programmodule **42**, **44**, **46** abgearbeitet, die die eigentlichen Funktionen der Frankiermaschine bewirken, wie z. B. das Eingeben von Daten, die Anzeige von Daten und das Drucken des Portowertes.

Nach dem Abarbeiten des Programmoduls DRUKKEN im Verfahrensschritt **46** wird wieder zum Verfahrensschritt **40** verzweigt, so daß die Funktionen der Frankiermaschine weiterhin aktiviert sind und bei Bedarf ausgeführt werden können. Das Starten und Abarbeiten der in den Verfahrensschritten **40** bis **46** genannten Programmodule muß nicht unbedingt in der in **Fig. 2** angegebenen Reihenfolge erfolgen, sondern kann je nach vorhandenem Betriebssystem interruptgesteuert in einer anderen, durch Anforderungen von außen vorgegebenen Reihenfolge ausgeführt werden.

Falls im Verfahrensschritt **38** festgestellt wird, daß die Zustandskennung ZK vor dem Spannungsausfall nicht den Wert 0 hat, d. h., daß ein kritischer Programmabschnitt unterbrochen wurde, so wird der Ablauf bei A fortgesetzt, der in **Fig. 3** dargestellt ist und nachfolgend beschrieben wird. Im Verfahrensschritt **50** wird abgefragt, ob die vor dem Spannungsausfall zuletzt abgespeicherte Zustandskennung ZK den Wert 1 hat. Falls dies zutrifft, so wird im Verfahrensschritt **52** die Zustandskennung ZK = 1 in den Bereich Z des Speichers **22** eingetragen, da der nachfolgende Programmschritt **54** sicherheitsrelevante Daten im Speicher **22** verändert und damit ein kritischer Programmabschnitt vorliegt. Bis zum Verfahrensschritt **52** hatte die aktuelle Zustandskennung ZK gemäß Verfahrensschritt **36** den Wert 0.

Der Wert 1 der vor dem Spannungsausfall zuletzt abgespeicherten Zustandskennung ZK-1 bedeutet, daß eine Unterbrechung des kritischen Programmabschnitts in der Phase erfolgt ist, in der Informationen in den ersten nicht flüchtigen Speicher, d. h. in den Bereich X, eingeschrieben oder verändert worden sind. Da im zweiten Speicher, d. h. im Bereich Y, sämtliche Informationen vom vorherigen Durchlaufen des kritischen Programmabschnitts noch unverändert erhalten sind, kann der vor der Spannungsunterbrechung im Bereich X herrschende Zustand wieder hergestellt werden. Hierzu werden gemäß Verfahrensschritt **54** die Informationen des Bereichs Y in den Bereich X übertragen.

Die nachfolgenden Verfahrensschritte betreffen wieder nicht kritische Programmabschnitte, s daß die Zustandskennung im Verfahrensschritt **56** auf den Wert 0 gesetzt wird. Im Verfahrensschritt **58** wird anhand der Modulkennung MK festgestellt, welches Programm - dul beim Spannungsausfall unterbrochen worden war. Je nach Art des unterbrochenen Programmoduls, werden die begonnenen Prozesse abgebrochen oder rück-

gängig gemacht. Beispielsweise wird eine teilweise bearbeitete Anforderung für ein Frankieren abgebrochen. Diese Frankieranforderung kann dann, falls noch erforderlich, erneut gestartet und bearbeitet werden. Erfolgte die Unterbrechung bei der Eingabe von Daten, so werden diese Daten ignoriert, und es wird gegebenenfalls erneut zur Eingabe von Daten aufgefordert. Anschließend wird zum Verfahrensschritt 40 verzweigt (Fig. 2) und die weiteren Programmodule abgearbeitet.

Wenn im Verfahrensschritt 50 festgestellt wird, daß der Wert der Zustandskennung ZK nicht 1 ist, was bedeutet, daß die Zustandskennung ZK den Wert 2 hat, so wird zum Verfahrensschritt 60 verzweigt. Der Wert 2 besagt einerseits, daß beim Spannungsausfall der kritische Programmabschnitt in der Phase unterbrochen worden ist, in der Informationen in den zweiten Speicher eingeschrieben worden sind. Andererseits sind die Informationen bei der Abarbeitung des kritischen Programmabschnitts noch ordnungsgemäß in den ersten Speicher eingetragen worden. Der Inhalt des zweiten Speichers muß demnach noch mit den Informationen des ersten Speichers beschrieben werden, damit beide Speicher identischen Inhalt haben. Da ein Speicherzugriff auf den Speicher 22 erforderlich ist und sicherheitsrelevante Daten geändert werden, wird im Verfahrensschritt 60 die aktuelle Zustandskennung ZK auf 2 gesetzt (sie hatte bislang den Wert 0) und im Verfahrensschritt 62 wird der Inhalt des Speicherbereichs X in den Bereich Y übertragen.

Mit dem nächsten Verfahrensschritt 64 beginnt wieder ein unkritischer Programmabschnitt in dem keine Daten im Speicher 22 geändert werden. Die Zustandskennung ZK wird daher im Verfahrensschritt 64 auf den Wert 0 gesetzt.

Im nachfolgenden Verfahrensschritt 66 wird anhand der Modulkennung MK festgestellt, welches Programmodul bearbeitet worden war, bevor die Unterbrechung infolge Spannungsausfalls aufgetreten ist. Da die Portoabrechnung im ersten nicht flüchtigen Speicher bzw. im Speicherbereich X ordnungsgemäß ausgeführt und damit die zu diesem Prozeßschritt gehörende Datenänderung im Speicher 22 erfolgreich durchgeführt worden ist, kann der unterbrochene Prozeß weitergeführt bzw. abgeschlossen werden. Beispielsweise kann eine begonnene und dann unterbrochene Frankierung nach Spannungswiederkehr zu Ende geführt werden. Anschließend wird zum Verfahrensschritt 40 (Fig. 2) weitergegangen.

In Fig. 4 ist der Ablauf beim Abarbeiten eines Programmoduls dargestellt, das kritische und nicht kritische Programmabschnitte enthält. Nach dem Start des Programmoduls wird die das Programmodul kennzeichnende Modulkennung MK in den Modulspeicher M eingetragen (Verfahrensschritt 70). Im darauffolgenden Verfahrensschritt wird als Zustandskennung ZK der Wert 0 in den Zustandsspeicher Z eingetragen und damit der nachfolgende Programmabschnitt als unkritisch gekennzeichnet. Beim Abarbeiten des nächsten Verfahrensschritts 74 werden die für die Funktion des Programmoduls notwendigen Berechnungen, die Prozeßsteuerung oder der Datentransfer durchgeführt, beispielsweise um einen Brief in der Frankiermaschine zu transportieren und zu frankieren.

Im Verfahrensschritt 76 wird abgefragt, b Inf rmationen im nicht flüchtigen Speicher 22 zu ändern sind. Falls dies nicht zutrifft, wird zum Schritt 88 verzweigt. Andernfalls werden die nachf lgenden Verfahrensschritte 78 bis 86 ausgeführt, die einen kritischen Programmabschnitt darstellen. Im Verfahrensschritt 78 wird die Zustandskennung ZK auf den Wert 1 gesetzt. Anschließend wird im Verfahrensschritt 80 die Manipulation des ersten nicht flüchtigen Speichers, d. h. im Speicherbereich X, ausgeführt und die Informationen eingeschrieben. Beispielsweise wird der nach einer durchgeführten Frankierung noch verbleibende Gesamtbetrag für das Porto eingetragen. Damit ist die erste Phase des kritischen Programmabschnitts abgeschlossen.

In der nachfolgenden zweiten Phase wird im Verfahrensschritt 82 die Zustandskennung ZK auf den Wert 2 gesetzt und anschließend im Verfahrensschritt 84 die vorgenannten Informationen in den zweiten nicht flüchtiger Speicher, d. h. in den Speicherbereich Y eingeschrieben. Damit ist die zweite Phase des kritischen Programmabschnitts abgeschlossen. Es ist noch zu erwähnen, daß während des kritischen Programmabschnitts auch Programmschritte wie z. B. Berechnungen oder Prozeßsteuerungen ausgeführt werden können. Die zum kritischen Programmabschnitt gehörenden Verfahrensschritte können in Form eines Unterprogramms oder eines Makroprogramms in das Programmodul eingebunden sein.

Nachfolgend wird im Verfahrensschritt 86 die Zustandskennung auf den Wert 0 gesetzt, der einen nachfolgenden unkritischen Programmabschnitt kennzeichnet. Im darauffolgenden Verfahrensschritt 88 wird überprüft, ob sämtliche Programmschritte des Programmoduls abgearbeitet sind. Wenn dies nicht zutrifft, so wird zum Verfahrensschritt 74 verzweigt. Andernfalls wird das nächste Programmodul abgearbeitet, z. B. das Programmodul des Verfahrensschritts 40.

In Fig. 5 sind in zwei Flußdiagrammen Verfahrensschritte dargestellt, die das mehrfache Einschreiben und Auslesen von Zustandskennungen betreffen. Diese Verfahrensschritte können auf analoge Weise auch beim Einschreiben und Lesen der Modulkennung verwendet werden. Wie weiter vorne bereits erläutert, dient das mehrfache Einschreiben dazu, die Redundanz des Verfahrens zu erhöhen, so daß fehlerhafte Zustandskennungen bei der Anwendung des Verfahrens toleriert werden. Die nachfolgend beschriebenen Verfahrensschritte 90 bis 98 sowie 100 bis 104 können beispielsweise an Stelle der Verfahrensschritte 78 (Fig. 4) bzw. 38 (Fig. 2) verwendet werden.

Im Verfahrensschritt 90 wird die aktuelle Zustandskennung, z. B. ZK = 1, in die Speicherzelle mit der Adresse einer Laufvariablen L des Zustandsspeichers Z eingeschrieben. Dieser Zustandsspeicher hat 4 Speicherzellen mit den Adressen A = 0, 1, 2, 3, 4. Die Laufvariable L hat beim ersten Einschreiben den Wert 0. Im nächsten Verfahrensschritt 92 wird unter Verwendung der Laufvariablen L auf die aktuelle Speicherzelle des Zustandspeichers Z zugegriffen und deren Inhalt gelesen. Im darauffolgenden Verfahrensschritt 94 wird überprüft, ob die Zustandskennung ZK richtig eingetragen worden ist. Wenn dies nicht der Fall ist, so wird zum Verfahrensschritt 90 verzweigt und der Schreibvorgang wiederholt. Falls die Zustandskennung erfolgreich in den Zustandsspeicher Z eingetragen wurde, wird im Verfahrensschritt 96 die Laufvariable um 1 erhöht.

Im Verfahrensschritt 98 wird geprüft, ob die Laufvariable L den Wert 4 erreicht hat. Bei negativem Ergebnis wird zu Schritt 90 verzweigt und die Eintragung in die Speicherzelle mit um 1 erhöhter Adresse ausgeführt. Bei positivem Ergebnis wird der Programmteil verlassen. Der Speicher Z enthält dann unter den Adressen A = 0

bis 4 die aktuelle Zustandskennung ZK.

Bei Spannungswiederkehr werden die Verfahrensschritte 100 bis 104 ausgeführt. Im Verfahrensschritt 100 werden die Speicherzellen mit den Adressen 0 bis 4 gelesen. Im nachfolgenden Verfahr nsschritt 102 wird eine Majoritäts- oder eine Plausibilitätsprüfung durchgeführt. Bei der Majoritätsprüfung wird festgestellt, welche Zustandskennung ZK am häufigsten in den vorgenannten Speicherzellen vorkommt. Diese Zustandskennung ZK wird dann im Schritt 104 als die letzte Zustandskennung ZK-1 verwendet. Bei der Plausibilitätsprüfung wird festgestellt, ob der oder die eingetragenen Werte einem gültigen, vorher festgelegten Wertebereich angehören, z. B. ZK = 0, 1, 2. Ist dies der Fall, so wird der zuletzt eingetragene gültige Wert als die letzte Zustandskennung ZK-1 verwendet.

Patentansprüche

1. Verfahren zum Betreiben einer Datenverarbeitungsanlage, bei dem die Datenverarbeitungsanlage mindestens einen kritischen Programmabschnitt abarbeitet, der das Einschreiben von Informationen in einen ersten nicht flüchtigen Speicher veranlaßt und der nach erfolgter Abarbeitung verlassen wird, wobei bei einer auf einen Spannungsausfall folgenden Spannungswiederkehr die vor dem Spannungsausfall im Speicher vorhandenen Informationen wieder bereitgestellt werden, dadurch gekennzeichnet, daß zu Beginn des Einschreibens der Informationen eine erste Zustandskennung (ZK = 1) in einen nicht flüchtigen Zustandsspeicher (Z) mindestens einmal eingeschrieben wird, daß nach dem Einschreiben der Informationen eine zweite, von der ersten Zustandskennung (ZK = 1) verschiedene Zustandskennung (ZK = 2) in den Zustandsspeicher (Z) mindestens einmal eingeschrieben wird, die selben Informationen in einen zweiten nicht flüchtigen Speicher (Y) eingeschrieben werden und der kritische Programmabschnitt verlassen wird, daß bei Spannungswiederkehr die vor dem Spannungsausfall in den Zustandsspeicher (Z) zuletzt eingeschriebene Zustandskennung (ZK-1) gelesen wird und bei Vorliegen der ersten Zustandskennung (ZK = 1) diese in den Zustandsspeicher (Z) mindestens einmal eingeschrieben wird, die Informationen aus dem zweiten Speicher (Y) in den ersten Speicher (X) übertragen werden und der kritische Programmabschnitt verlassen wird, und daß bei Vorliegen der zweiten Zustandskennung (ZK = 2) diese in den Zustandsspeicher (Z) mindestens einmal eingeschrieben wird, die Informationen aus dem ersten Speicher (X) in den zweiten Speicher (Y) eingelesen werden und der kritische Programmabschnitt verlassen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Datenverarbeitungsanlage (10) weiterhin mindestens einen unkritischen Programmabschnitt abarbeitet, der kein Einschreiben von Informationen in den ersten oder zweiten nicht flüchtigen Speicher (X) veranlaßt, wobei zu Beginn des Abarbeitens dieses unkritischen Programmabschnitts in den Zustandsspeicher (Z) eine dritte Zustandskennung (ZK = 0) mindestens einmal eingeschrieben wird, und daß bei Spannungswiederkehr beim V rliegen der dritten Zustandskennung (ZK = 0) das Abarbeiten des unkritischen Programmabschnitts beim unterbrochenen Programmschritt fortgesetzt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß mindestens ein kritischer Pr - grammabschnitt und/oder mindestens ein unkritischer Programmabschnitt Teil eines Programmoduls ist, das von der Datenverarbeitungsanlage (10) abgearbeitet wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß nach Spannungswiederkehr und bei Vorliegen der ersten Zustandskennung (ZK = 1) die vom Programmodul gesteuerten Prozesse zurückgesetzt und/oder das Programmodul erneut abgearbeitet wird.

5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß nach Spannungswiederkehr und bei Vorliegen der zweiten Zustandskennung (ZK = 2) das Abarbeiten des Programmoduls fortges tzt wird.

6. Verfahren nach einem der Ansprüche 3 bis 5, dadurch gekennzeichnet, daß beim Abarbeiten mehrerer Programmodule jedem Programmodul eine Modulkennung (MK) zugeordnet wird, die in einem nicht flüchtigen Modulspeicher (M) zu Beginn des Abarbeitens des Programmoduls mindestens einmal abgespeichert wird, und daß bei Spannungswiederkehr zum Programmodul mit der zuletzt abgespeicherten Modulkennung (MK) verzweigt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß ein nicht flüchtiger Zentralspeicher (22) eingesetzt wird, dessen verschiedenen, voneinander getrennten Speicherbereiche als erster, zweiter nichtflüchtiger Speicher (X, Y) bzw. als Zustandsspeicher (Z) verwendet werden.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß ein Speicherbereich (M) des Zentralspeichers (22) als Modulspeicher verwendet wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die erste, die zweite und/oder die dritte Zustandskennung (ZK = 1, 2, 0) und/oder die Modulkennung (MK) jeweils in n Speicherzellen des jeweiligen Speichers (Z bzw. M) mehrfach abgespeichert wird, wobei n eine vorgegebene Zahl ist, vorzugsweise 3.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, daß bei Spannungswiederkehr die n Speicherzellen der jeweiligen Speicher (Z bzw. M) gelesen werden, und daß durch eine Majoritätsprüfung und/oder eine Plausibilitätsprüfung festgestellt wird, welche Zustandskennung (ZK) bzw. Modulkennung (MK) vorliegt.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es in einer Frankiermaschine angewendet wird.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, daß beim Abarbeiten des kritischen Programmabschnitts die Portoabrechnung durchgeführt wird.

13. Verfahren nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß bei der Abarbeitung des unkritischen Programmabschnitts der Druckvorgang beim Frankieren ausgeführt wird.

Hierzu 5 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 42 17 830 A1
Int. Cl.[5]: G 06 F 1/30
Offenlegungstag: 2. Dezember 1993

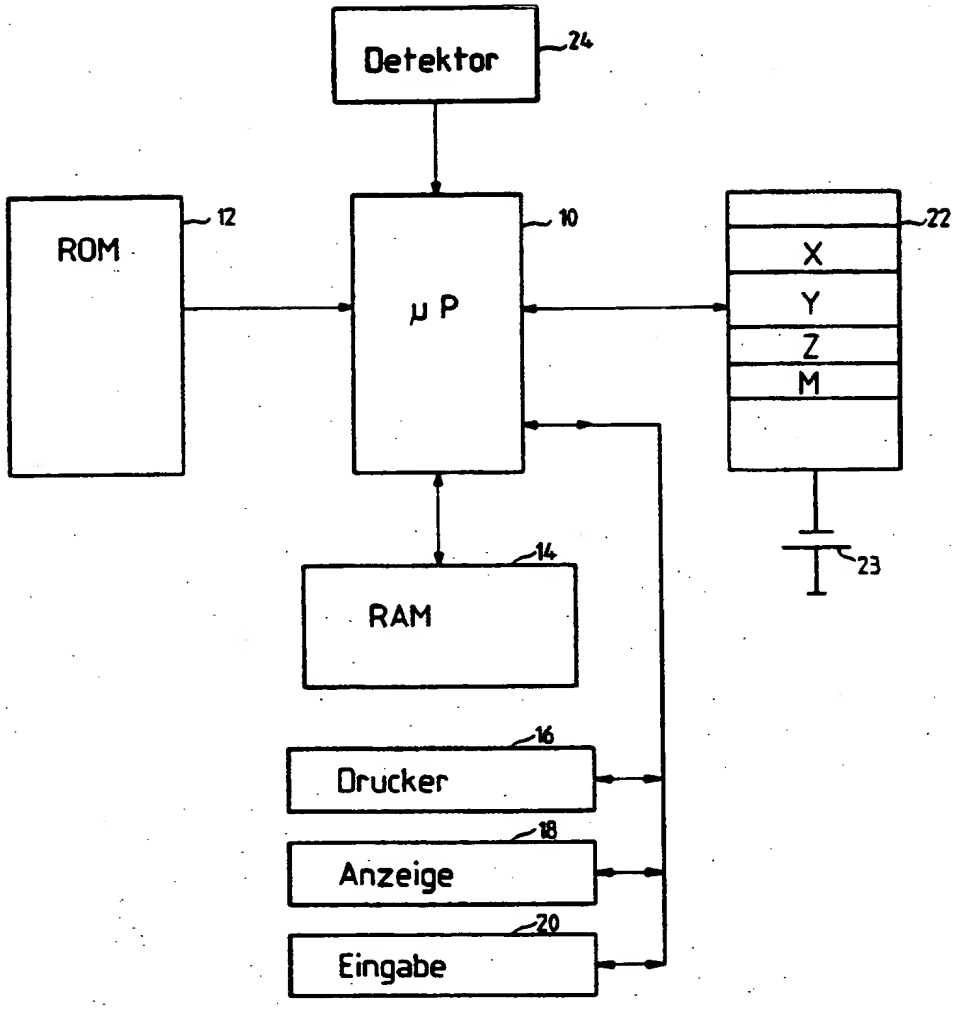


Fig. 1

Nummer: DE 42 17 830 A1
Int. Cl.[5]: G 06 F 1/30
Offenlegungstag: 2. Dez mber 1993

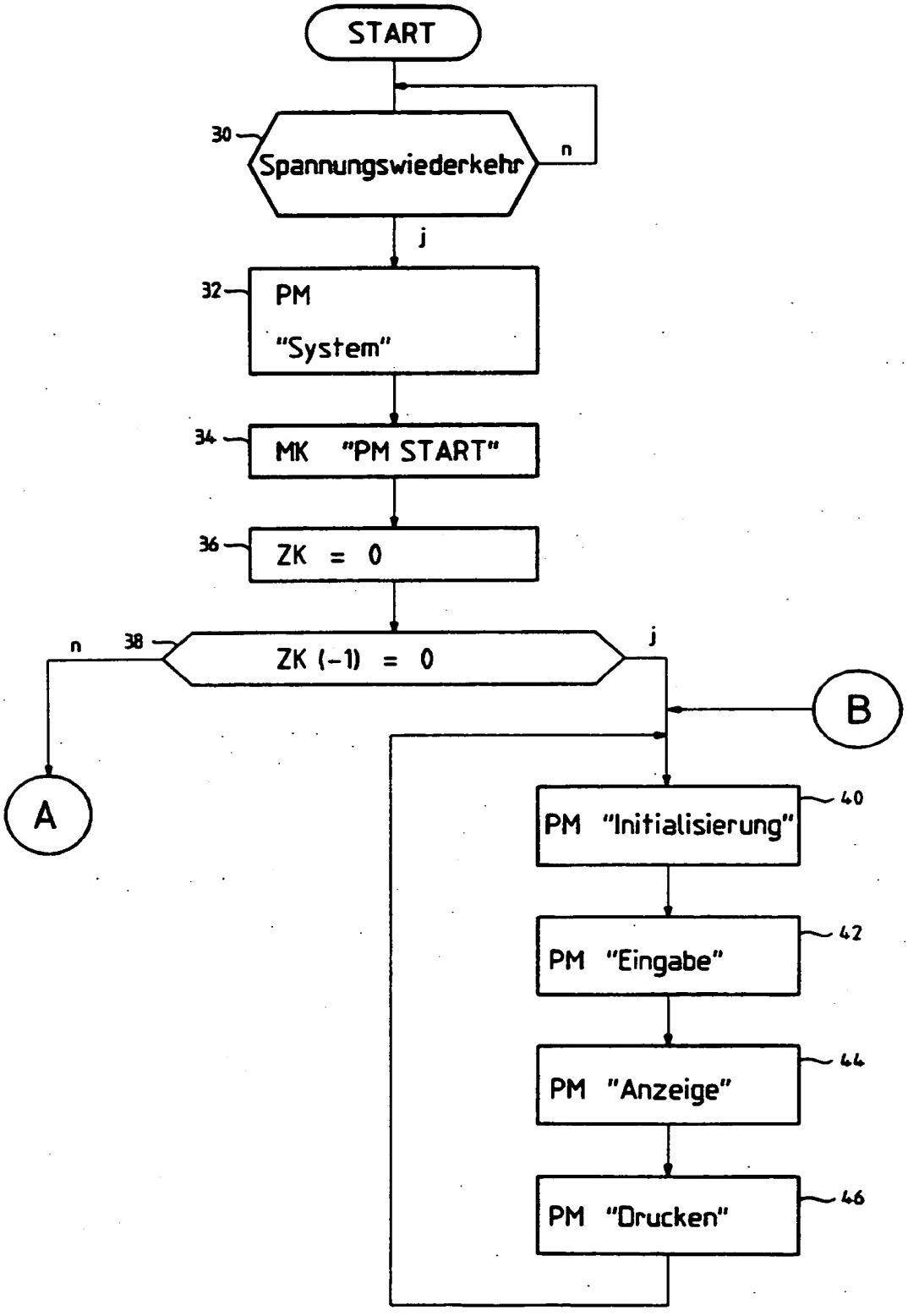


Fig. 2

Nummer: DE 42 17 830 A1
Int. Cl.[5]: G 06 F 1/30
Offenlegungstag: 2. D zember 1993

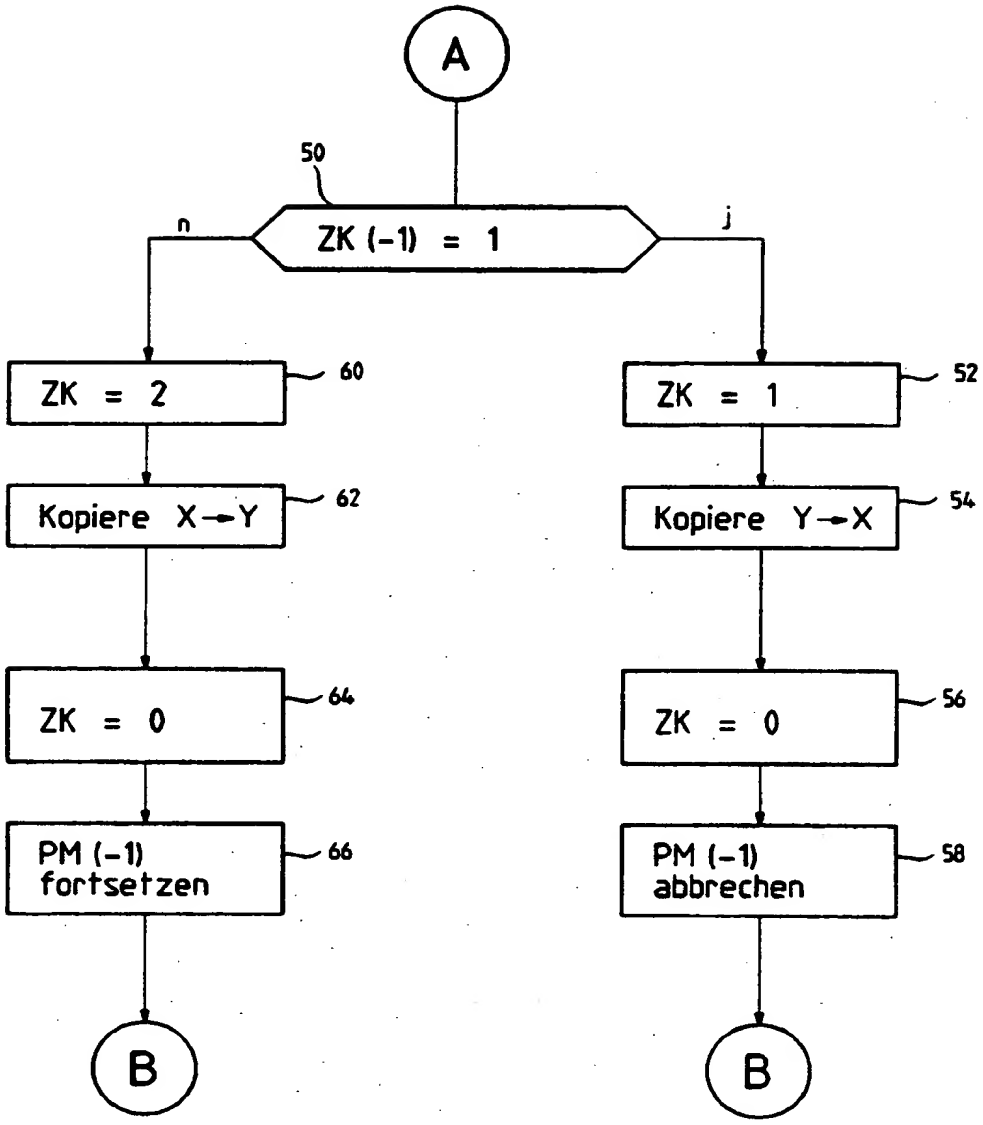


Fig. 3

Nummer: DE 42 17 830 A1
Int. Cl.[5]: G 06 F 1/30
Offenlegungstag: 2. Dezember 1993

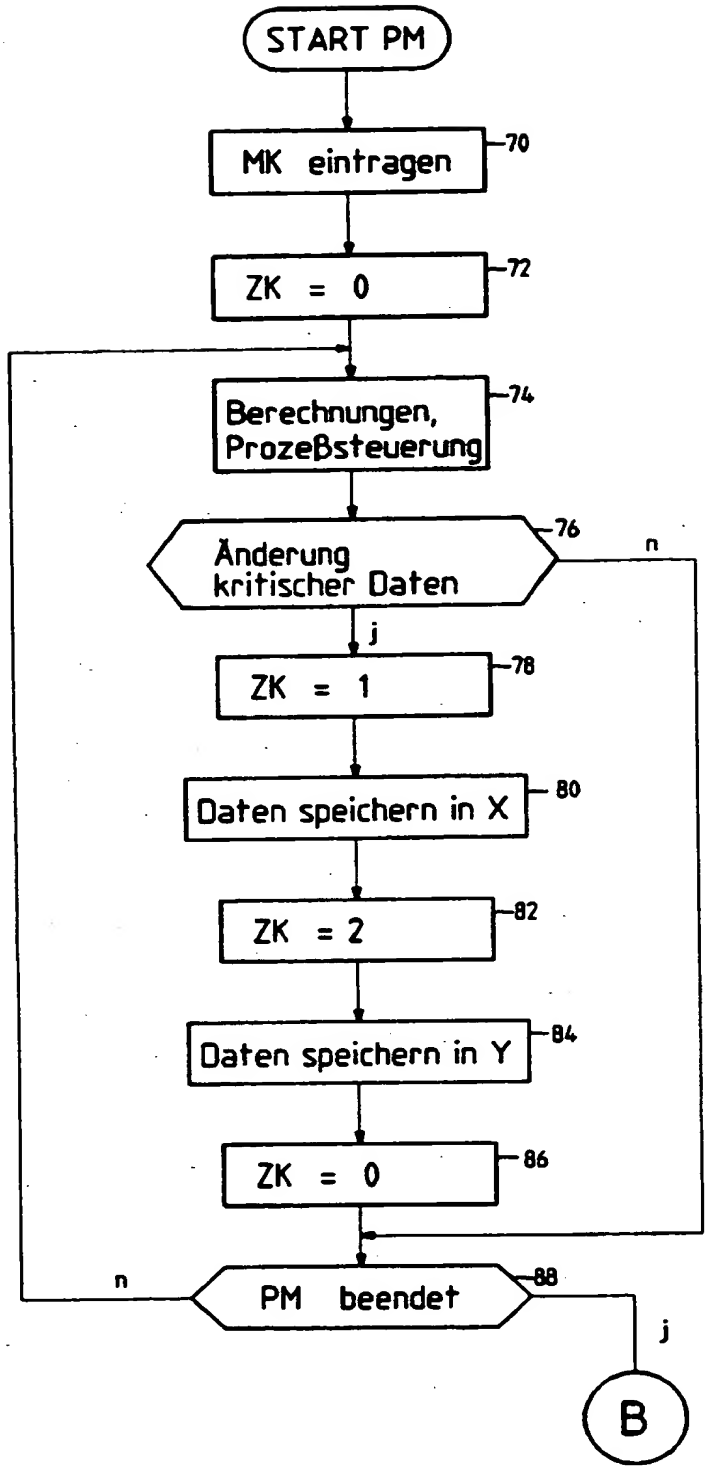
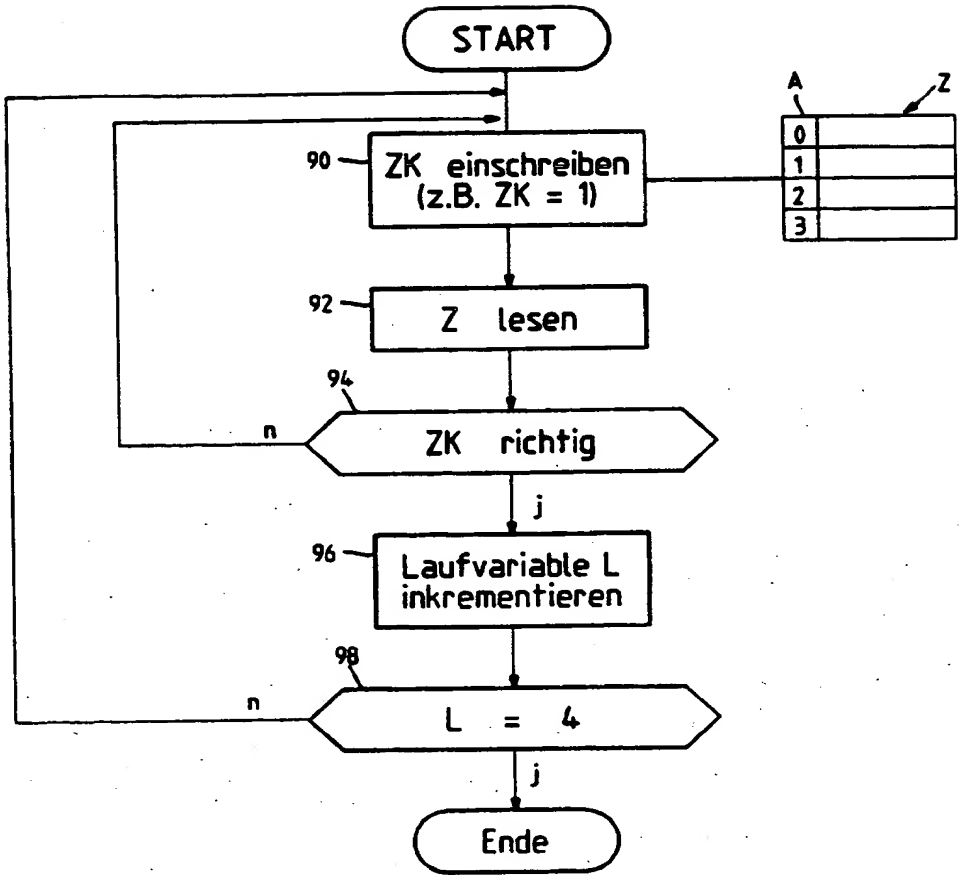


Fig. 4

Numm r: DE 42 17 830 A1
Int. Cl.[5]: G 06 F 1/30
Offenlegungstag: 2. Dezember 1993



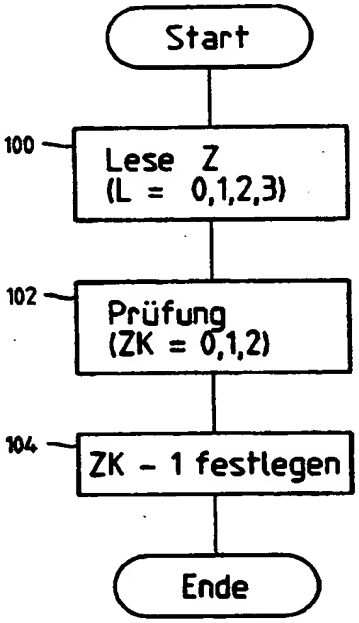


Fig. 5

1/5/1
DIALOG(R)File 351:DERWENT WPI
(c) 2000 Derwent Info Ltd. All rts. reserv.

009685388 **Image available**
WPI Acc No: 93-378942/199348
XRPX Acc No: N93-292643
Data processor operating system - stores data in ROM during critical program step to ensure memory back-up of information for critical program step to prevent loss upon voltage supply failure
Patent Assignee: FRANCOTYP POSTALIA GMBH (FRAN-N); FRANCOTYP-POSTALIA & CO AG (FRAN-N)
Inventor: GUENTER S; GUENTHER S
Number of Countries: 017 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 572019	A2	19931201	EP 93108608	A	19930527	G06F-011/14	199348 B
DE 4217830	A1	19931202	DE 4217830	A	19920529	G06F-001/30	199349
EP 572019	A3	19941130	EP 93108608	A	19930527	G06F-011/14	199536
DE 4217830	C2	19960118	DE 4217830	A	19920529	G06F-001/30	199607
EP 572019	B1	19980812	EP 93108608	A	19930527	G06F-011/14	199836
DE 59308855	G	19980917	DE 508855	A	19930527	G06F-011/14	199843
			EP 93108608	A	19930527		

Priority Applications (No Type Date): DE 4217830 A 19920529
Cited Patents: No-SR.Pub; 1.Jnl.Ref; EP 249061; WO 8402409
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
EP 572019	A2	G	13			
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE						
DE 4217830	A1		11			
DE 4217830	C2		11			
EP 572019	B1	G				
Designated States (Regional): CH DE FR GB IT LI						
DE 59308855	G			Based on		EP 572019

Abstract (Basic): EP 572019 A

The operating system allows information entered in a memory before a temporary interruption in the voltage supply to be recovered when the voltage is restored. The data processor has a read-only memory in which information is entered during a critical programme step, a random access memory and a second read-only memory holding condition information.

A condition indication is supplied to the latter memory upon initiating write-in of information to the first read-only memory, a second condition information supplied at the end of the information write-in, before the same information is fed to the random access memory and the critical programme step performed. The condition information is used to access the information upon a voltage interruption.

ADVANTAGE - Ensures memory back-up so no data loss upon power failure.

Dwg.1/5

Title Terms: DATA; PROCESSOR; OPERATE; SYSTEM; STORAGE; DATA; ROM; CRITICAL ; PROGRAM; STEP; ENSURE; MEMORY; BACK-UP; INFORMATION; CRITICAL; PROGRAM; STEP; PREVENT; LOSS; VOLTAGE; SUPPLY; FAIL
Derwent Class: T01
International Patent Class (Main): G06F-001/30; G06F-011/14
International Patent Class (Additional): G06F-012/16; G07B-017/00
File Segment: EPI